Nevada Department of Education (NDE)

Information Security and Privacy Policy

I. Purpose

"If our destination is improved student achievement, we cannot get there without valuing and effectively using data in education" (Data Quality Campaign, Roadmap to Safeguarding Student Data: http://www.dataqualitycampaign.org/find-resources/roadmap-for-safeguarding-student-data/).

The state believes it is critical to collect and use student and educator data to continuously improve education services, provide system transparency, and ensure that educators and families have access to high quality data no matter where they live.

Data collection assists administrators, leaders, businesses, government agencies, and legislators to provide the most efficient and cost effective system which meets the needs of our students throughout the state. Most importantly, these data allows policy planners and educational staff to meet the specific needs of all students in the most objective manner by closing achievement gaps and overcoming differences of gender and ethnicity. Another important use of data is to empower parents with information to ensure that their child is getting what he or she needs.

The effective, meaningful use of education data to improve student achievement requires proper safeguards to ensure the safety and security of these data. The publishing of data results provides a means for all concerned citizens, as well as our elected and appointed leaders, to know where we are doing well and where we need to do better. Currently available data reports are located on the Nevada Department of Education website (http://www.doe.nv.gov/DataCenter/) providing access to information such as the Nevada Report Card, Nevada School Performance Framework, and other useful school and program results.

II. Overview

The Nevada Department of Education (NDE) considers it our moral and legal responsibility to protect student privacy and ensure data security and confidentiality. We value the use of data in improving student achievement and system performance in our state. We also understand how vital it is to ensure those data are accessed and used appropriately by creating clear policies around data security.

The NDE only collects data in accordance with law and regulation, and access is limited and appropriate. Any student and educator data collected and stored by NDE is, at all times, under the control of the NDE. The NDE has the final say in how data are shared pursuant to the provisions in law, regulation, and FERPA. The data the NDE collects meet specific policy, practice, and service needs, and only authorized persons are allowed to access. Additionally, any student level data the NDE collects is a sub-set of student information collected at each of the state's school districts and charter schools.

The Federal Educational Rights and Privacy Act (FERPA) is a federal regulation which provides a baseline for protecting student privacy. We consider FERPA the floor for protecting student privacy, not the ceiling. FERPA provides parameters for what is permissible when sharing student information. The law does not prohibit sharing data across agencies. The state has implemented policies and procedures above and beyond FERPA to manage our data and protect student privacy.

The responsibility to protect student data is system-wide. While the state must play a leadership role in data security policies; districts, schools, and their staff also have a responsibility to adhere to these policies and be good stewards of student data. To that end, the NDE created the Data Collaborative. The Data Collaborative is an internal organization comprised of NDE staff and is responsible for data governance and NDE processes created to ensure current and historical student, teacher, schools, and control data are formally managed throughout the NDE.

The NDE, under the guidance of the State Department of Enterprise Information Technology's Office of Information Security, follows the State Information Security Policy standards and is a member of the State Security Policy Committee. The State Information Security Policy was developed based on the International Standard (ISO/IEC 27002:2005) Code of Practice for Information Security Management and the National Institute of Standards and Technology (NIST Publication 800). Compliance with the State Information Security Policies is mandatory for all agencies in the Executive Branch of Nevada State Government with the exception of the Nevada System of Higher Education (NSHE) and the Nevada Criminal Justice Information Computer System. In cases where entities cannot comply with any section of the State Information Security Policy, an exception request must be documented, all potential risks identified and submitted to the Office of Information Security for approval.

More information about the consolidated State Information Security Policy can be located at: http://it.nv.gov/uploadedFiles/ITnvgov/Content/Governance/dtls/Standards/4.100000StateConsolidatedPolicy.pdf

III. Internal Process for Maintaining the Information and Security Policy

In conjunction with the U.S. Department of Education's Privacy Technical Assistance Center and the NDE's Data Collaborative, NDE annually monitors changes in state and federal regulations that are related to data collection and reporting and updates the NDE procedures to address any new requirements and best practices. For instance, FERPA was recently reauthorized (in January 2012) to include additional clarity around and support the development and use of statewide longitudinal data systems. NDE's policies and procedures have been reviewed by NDE staff, the Data Collaborative, and legal counsel to ensure that they fully align with these revised federal regulations.

IV. Access to Student Information

Nevada Revised Statutes (NRS) 386.650 requires that the NDE "shall establish, to the extent authorized by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (FERPA), and any regulations adopted pursuant thereto, a mechanism by which persons or entities, including, without limitation, state officers who are members of the Executive or Legislative Branch, administrators of public schools and school districts, teachers and other educational personnel, and parents and guardians, will have different types of access to the accountability information contained within the automated system to the extent that such information is necessary for the performance of a duty or to the extent that such information may be made available to the general public without posing a threat to the confidentiality of an individual pupil." This statute is the primary mechanism for guiding such access. To comply with state law, the NDE provides a series of accountability reports, including but not limited to the Nevada Report Card and the Nevada School Performance Framework, designed to give state and local officials, educators, parents, and other stakeholders access to aggregated, de-identified accountability information.

FERPA gives parents the right to review and confirm the accuracy of their child's education records maintained by NDE. This includes, for example, state assessments administered by the school districts and maintained by NDE. These rights transfer to the student when the student turns 18 years old or attends a postsecondary institution. NDE must comply with a parent's request to inspect and review education records within a reasonable period of time, but not more than forty-five days after it has received a request. NDE may make the education records available to the parent either directly, by sending them to the local school district for inspection and review, or making other appropriate arrangements. FERPA generally permits NDE to charge a fee for a copy of an education record made for a parent, unless imposing a fee effectively prevents a parent from exercising his or her right to inspect and review records.

FERPA requires NDE to use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses personally identifiable information from education records. NDE may ask for legal certification denoting parenthood, such as a birth certificate, as well as for other forms of identification if needed. Alternatively, NDE may work with the local school district or school to verify the requestor's status as the child's parent.

V. Staff Training

In order to minimize the risk of human error and misuse of information, NDE provides a range of training opportunities for all staff using educational data and adheres to the state's Information Security Program as established by the Nevada State Information Security Committee.

All NDE employees must sign and adhere to the NDE's Acceptable Use Policy, which describes the permissible uses of state technology and information, and participate in the security awareness training provided by the state. All NDE employees must also sign and adhere to the NDE Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data. Employees are required to participate in and annual information security and privacy fundamentals training, which is mandatory for continued access to the NDE's network.

Additionally, NDE requires targeted information security training for specific groups within the agency such as system administrators and other technical personnel, and provides updated guidance to school districts concerning compliance with state and federal privacy laws and best practices.

VI. Internal Use of Data

The personally identifiable information from students' and educators' records that NDE receives from districts, charter schools, and schools for audit, evaluation, or compliance purposes is not available to all NDE employees. This information is only available to employees who have undergone a background check and who have a reasonable and appropriate need for access to the information in order to maintain the records or to assist in conducting NDE evaluation, audit, or compliance functions. The NDE's Data Collaborative is comprised of staff at NDE who helps ensure that data is properly handled from collection to reporting. This committee assists in identifying NDE employees who have a legitimate need for access to data and developing and maintaining policies concerning the management of the NDE's data. The committee also provides the Superintendent or Deputy Superintendent with an up-to-date list of the specific individuals within the NDE who have the ability to link personally identifiable student and educator information.

NDE utilizes various procedures and security measures to ensure the confidentiality of pupil records. These procedures include assignment of a unique identifier to each pupil and statistical cutoff procedures. A unique pupil identification number (ID) is assigned to each Nevada pupil. The ID is computer-generated and contains no embedded meaning. After being checked for duplicates, the ID becomes permanently assigned to the pupil. The NDE uses the "n" size of 10 for statistical cutoff procedures for data that is confidentially maintained. This applies to all aggregation reporting that is based on confidential data.

VII. Breaches in Security

Concerns about security breaches must be reported immediately to the NDE's Director of Information Technology. If the Director, in collaboration with NDE's Information Security Officer, determines that one or more employees or contracted partners have substantially failed to comply with the NDE's information security and privacy policies, he/she will report the incident to the Superintendent and Nevada's Office of Information Security. Consequences for a breach in security may include termination of employment or a

contract and further legal action. Concerns about security breaches that involve the Director of Information Technology must be reported immediately to the Information Security Officer and the Superintendent. The Superintendent and the Information Security Officer will collaborate with the Office of Information Security to determine whether a security breach has occurred and will identify appropriate consequences, which may include termination of employment or a contract.

VIII. Disclosure of Educator Data

The NDE is responsible for several activities that require the collection of data for licensed educators in Nevada. As the entity responsible for issuing and renewing educator licenses, linking student achievement to practicing educators, and monitoring implementation of local educator evaluation systems; NDE must manage and secure information that is sensitive and confidential. The NDE maintains several statutory and regulatory protections to keep educator data private.

Except as otherwise provided in NRS 239.0115, files relating to the application, including the applicant's health records, fingerprints and any report from the Federal Bureau of Investigation or the Central Repository for Nevada Records of Criminal History, transcripts, scores on examinations as required by the Commission, correspondence concerning the application, and any other personal information are classified as confidential (NRS 391.035; personal information is defined in NRS 603A). Each educator has the right to inspect and to have copies made (at the educator's expense) of all information pertaining to the educator. Educators may challenge any such record by formal letter or other evidence, which shall be added to NDE's records. The information may be shared in the normal and proper course of administering licenses and authorizations, but it is otherwise unlawful for any NDE employee or other person to divulge, or make known in any way, any such personal information without the written consent of the educator. Personnel information may be published in the aggregate, so long as the identities of individual educators remain anonymous and the data pool is large enough to prevent the identification of individual educators, which in no instance shall be smaller than ten (10) educators.

NRS 386.650 clarifies that, while NDE may collect information concerning an individual educator and student assessment results linked to that educator/classroom in order to fulfill duties as required by law, this information may, at the NDE's discretion, be shared so long as the confidentiality of each individual pupil is protected.

IX. Disclosure of De-identified or Anonymous Student Data

NDE may disclose de-identified student data through the process outlined by the NDE's Data Collaborative. The Data Collaborative considers and reviews all requests to conduct research using Nevada student or school system data already collected by NDE. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit proposals before receiving data and conducting and publishing their research.

The Data Collaborative considers and reviews all requests to conduct research using Nevada student or school system data that will require additional data collection (i.e., not already collected by NDE). In the event of such a request the Data Collaborative will determine the feasibility of such a collection and forward the request with an analysis and recommendation to the Superintendent for review and approval or denial of such a request.

Based on each data request, the NDE's Data Collaborative ensures that any data shared is "de-identified" (so that individual students are not personally identifiable). For instance, data may be considered "de-identified" if a meaningless code has been attached to each student's record in a way that prevents any student's identity

from being discovered or the data has been aggregated into a large enough pool of data that a student's identify cannot be inferred.

Those requesting data must meet all of the Data Collaborative criteria prior to obtaining access to any de-identified student-level data from NDE. One of these criteria is that the researchers have completed training on the ethical and professional standards for protecting human research participants that is either the same as or equivalent to the training that NDE employees complete.

For more information about how de-identified student data may be disclosed, see the NDE Data Request Form and process.

X. Disclosure of Personally Identifiable Student Data

NDE reserves the right to disclose data that it maintains; the data will be released at the discretion of NDE even if the disclosure would fall under one of the FERPA exceptions. In compliance with FERPA and state law, NDE will not disclose personally identifiable information from student records unless the disclosure is for one of the limited purposes outlined in FERPA, 34 CFR § 99.31, including the following:

- Use by School Officials for Legitimate Educational Purpose: Student information may be disclosed to school officials who have legitimate educational interests. A school official has a legitimate educational interest if the official needs to review an educational record in order to fulfill his or her professional responsibility.

- Student Transfer and Enrollment: Student information may be disclosed, subject to the requirements of FERPA, 34 CFR § 99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer and the student's former district has provided prior notification of this service through its annual FERPA notification letter.

- Educational Studies: (see 20 U.S.C. §1232g(b)(1)(F) and §99.31(a)(6)) Student information may be disclosed to organizations conducting studies for, or on behalf of, NDE to: (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction. Disclosures for the purposes of such studies must ensure that the study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information, the information is destroyed when no longer needed for the purposes for which the study was conducted, and NDE enters into a written agreement that meets the requirements outlined below.

- Evaluating/Auditing or Compliance Activities: (see 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5) and §§99.31(a)(3) and 99.35) Student information may be disclosed to authorized representatives of NDE in connection with an audit or evaluation of Federal or state supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. Disclosures for the purposes of such audits, evaluations, or compliance activities must ensure that NDE uses reasonable methods to ensure that its authorized representative: (1) uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs; (2) protects the personally identifiable information from further disclosures or other uses, in accordance with FERPA; (3) destroys the personally identifiable information in accordance with FERPA; and (4) NDE enters into a written agreement that meets the requirements outlined below.

XI. Requirements for Data Sharing Agreements to Disclose Student Data for Studies on Behalf of NDE

Prior to sharing personally identifiable student information for purposes of educational studies for or on behalf of NDE, NDE must enter into a written agreement or contract that meets the following requirements:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question;

- Specifies the purpose, scope and duration of the study and the information to be disclosed. This description must include the research methodology and why disclosure of personally identifiable information from education records is necessary to accomplish the research. Note, NDE will not disclose all of the personally identifiable information from its education records; rather, it will determine only the specific elements the authorized representative needs and disclose only those;

- Requires the authorized representative to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for further disclosure, unless authorized. Approval to use the personally identifiable information from the education records for one study, audit, or evaluation does not confer approval to use it for another;

- Requires the authorized representative to conduct the study in a manner that does not permit the personal identification for parents and students by anyone other than representatives of the organization with legitimate interests. The agreement must require the authorized representative to conduct the study so as to not identify students or their parents. This typically means that the authorized representative should allow internal access to personally identifiable information from education records only to individuals with a need to know for the purposes of the study, and that the authorized representative will take steps to maintain the confidentiality of the personally identifiable information at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques;

- Affirms that the authorized representative may only publish results in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance must be used so that students cannot be identified through small numbers displayed in table cells;

- Requires the authorized representative to destroy the personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP") and hyper-text transfer protocol over secure socket layer ("HTTPS"). The agreement establishes policies and procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information to only the authorized representatives with a legitimate interests in the research or study; and

- Includes a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to NDE.

XII. Requirements for Data Sharing Agreements to Disclose Student Data for Audits, Evaluation or Compliance Monitoring

Written agreements for audits, evaluation or compliance monitoring are similar to, but slightly different than, agreements for research and studies. These written agreements or contracts must include the following requirements:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question;

- Specifies the purpose for which the personally identifiable student information from education records is being disclosed and state specifically that the disclosure is in furtherance of an audit, evaluation, or enforcement or compliance activity. The agreement must specify the student information to be disclosed and must include a description of how the student data will be used. The agreement must describe the methodology and why disclosure of personally identifiable student information is necessary to carry out the audit, evaluation, or enforcement or compliance activity;

- Requires the authorized representative to destroy the personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP") and hyper-text transfer protocol over secure socket layer ("HTTPS"). The agreement establishes policies and procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information to only the authorized representatives with a legitimate interests in the audit, evaluation, or enforcement or compliance activity; and

- Includes a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to NDE.

XIII. Monitoring Implementation of Data Sharing Agreements

In addition to all of the precautions addressed above, any data sharing agreement or contract shall also address the following assurances to protect personally identifiable information from further disclosure and unauthorized use:

- NDE shall verify that the authorized representative has in place a data stewardship plan with support and participation from across the organization that details the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction. NDE may also wish to verify that the authorized representative has a training program to teach its employees about FERPA and how to protect personally identifiable information from education records; NDE shall maintain the right to conduct audits or other monitoring activities of the authorized representative's policies, procedures, and systems;

- NDE shall verify that the authorized representative has a sound data security program to protect data at rest and in transmission. This may be addressed through language in the data sharing agreement that states what data security provisions are required, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access. This also may include the right for NDE to physically inspect the authorized representative's premises or technology used to transmit or maintain data;

- If applicable, NDE shall verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances;

- NDE shall maintain the right to conduct audits or other monitoring activities of the authorized representative's policies, procedures, and systems; and

- NDE shall maintain the right to review any data prior to publication and to verify that proper disclosure avoidance techniques have been used and shall maintain the right to approve reports prior to publication to ensure they reflect the original intent of the agreement.

XIV. Consequences for Failure to Comply with Data Sharing Agreements

An individual may file a written complaint with NDE regarding an alleged violation of a data sharing agreement or contract. A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. NDE will investigate all reasonable and timely complaints following the procedure outlined under Security Breaches. NDE, in collaboration with the Office of Information Security, may also conduct its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether a violation has occurred.

As required by FERPA, if an authorized representative that receives data to perform evaluations, audits, or compliance activities improperly discloses the data, NDE shall deny that representative further access to personally identifiable data for at least five years. In addition, NDE may pursue penalties permitted under state contract law, such as liquidated damages.

XV. Additional Resources

NDE maintains and enforces a series of other policies related to information security, including:

- State-Level Student Data Collection and Protection;
- CDE Guidelines for Data Requests; and
- District Guidance: Information Security and Privacy.

Additional resources related to the collection, storage and safeguarding of student and educator information, including links to resources published by Education Privacy Information Center, the Data Quality Campaign, Fordham Center on Law and Information Policy, and the Privacy Technical Assistance Center, are available at http://www.doe.nv.gov/DataCenter/Student_Data_Privacy/.

Questions

Questions about the Information Security and Privacy Policy at the Nevada Department of Education should be directed to Glenn Meyer, Director Information Technology or Cindy Lou Little, Information Security Officer.

Statutes of Interest

NRS 386.650 Adoption and maintenance of system; adoption of uniform program for school districts to collect, maintain and transfer data to system; duties of Superintendent of Public Instruction; access to data within system.

NRS 386.655 Operation of system; compliance with federal law governing release and confidentiality of records

NRS 388.483 Pupils with autism spectrum disorder: Department required to submit annual report to Aging and Disability Services Division

NRS 392.456 Form for use in elementary schools concerning status of pupil and participation of parent; restrictions on use

NRS 392C.010 Enactment of Compact; text of The Interstate Compact on Educational Opportunity for Military Children

NRS 385.347 Program of accountability for school districts and charter schools; preparation of annual report of accountability by school districts and sponsors of charter schools; public dissemination of report; notice of availability on Internet. [Parts of this section were replaced in revision in 2013 by NRS 385.3472, 385.3474, 385.3476, 385.3478, 385.3481, 385.3483, 385.3485, 385.3487, 385.3489, 385.3491, 385.3493 and 385.3495.]

NRS 385.3572 State accountability report: Requirements; public dissemination of report; notice of availability on Internet

NRS 388.5317 Annual report by school districts on use of restraint and violations; compilation of reports by Department; submission of compilation to Legislature

NAC 388.289 Confidentiality of records. (NRS 385.080, 388.520)

NAC 388.292 Notice of project to identify, locate or evaluate pupils or educational data. (NRS 385.080, 388.520)

NAC 388.310 Resolution of dispute by hearing. (NRS 385.080, 388.520)

NAC 388.315 Appeal from decision of hearing officer. (NRS 385.080, 388.520)

NRS 394.379 Annual report by private schools on use of restraint and violations; compilation of reports by Department; submission of compilation to Legislature

NRS 396.535 Form required for informed consent of students concerning release or disclosure of personally identifiable information

NAC 392.325 "Personally identifiable information" defined.

NAC 392.350 Confidentiality of personally identifiable information; maintenance of permanent record; disclosure under certain circumstances. (NRS 385.080, 392.029)

Many of the above statutes or regulations refer to FERPA. Under the federal regulations adopted pursuant to FERPA, "personally identifiable information" includes but is not limited to the following:

"(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates."